

CHECKLISTE ÜBER SICHERHEIT IN LIEFERKETTEN

Supply Chain Security im Behörden- sowie Unternehmensumfeld

ID	AKTIVITÄT	STATUS		
I	ALLGEMEINE ASPEKTE DER SUPPLY CHAIN SECURITY			
01	Ist in Ihrer Organisation ein organisationsweites Informationssicherheitsmanagementsystem (ISMS) etabliert, in Betrieb und wird dieses kontinuierlich verbessert?	OK	KO	N/A
02	Sind Prozesse an Externe ausgelagert („Outsourcing“)?	OK	KO	N/A
03	Sind sicherheitsrelevante Prozesse an Externe ausgelagert?	OK	KO	N/A
04	Erfolgt eine regelmäßige Kontrolle der ausgelagerten Prozesse?	OK	KO	N/A
05	Bezieht Ihre Organisation externe Güter, Produkte oder Dienstleistungen?	OK	KO	N/A
06	Bezieht Ihre Organisation sicherheitsrelevante externe Güter, Produkte oder Dienstleistungen?	OK	KO	N/A
07	Erfolgt eine Dokumentation der Prozesse die ausgelagert sind oder der extern bezogenen Güter, Produkte bzw. Dienstleistungen?	OK	KO	N/A
08	Führt Ihre Organisation eine Unterscheidung durch, ob ein Prozess vollständig oder teilweise ausgelagert wird?	OK	KO	N/A
09	Gibt es Produkte oder Dienstleistungen, die Ihre Organisation von Zulieferern bezieht und welche zu einem späteren Zeitpunkt entweder von anderen Zulieferern oder Ihrer Organisation selbst zusammengesetzt oder montiert werden?	OK	KO	N/A
10	Berücksichtigt Ihre Organisation im Rahmen des Risikomanagements Informationssicherheits-Risiken in der Supply Chain?	OK	KO	N/A
II	TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN			
11	Gibt es eine Richtlinie für das Management der Lieferantenbeziehungen? Behandelt diese Richtlinie insbesondere Aspekte von Verkettungen von Dienstleistern bzw. die Abhängigkeiten von weiteren Dritten, die etwa als Dienstleister für Ihre Dienstleister tätig sind? Werden damit verbundene Schwachstellen (z.B. Single-Point-of-Failures die nicht beim ersten Dienstleister sondern weitere Ebenen dahinter liegen) berücksichtigt?	OK	KO	N/A
12	Verfügt Ihre Organisation über einen Prozess zum Management von Risiken?	OK	KO	N/A
13	Verfügt Ihre Organisation über einen Prozess zum Management von Risiken in Verbindung mit der Sicherheit von Lieferketten?	OK	KO	N/A
14	Werden Listen aller zuliefernden Organisation erstellt und gewartet?	OK	KO	N/A
15	Gibt es Alternativen für die zuliefernden Betriebe bzw. Organisationen und sind diese geeignet dokumentiert bzw. gewartet?	OK	KO	N/A
16	Sind Zulieferbetriebe bzw. Organisationen oder deren Mitarbeiterinnen bzw. Mitarbeiter in das Rollen- und Rechtmanagement Ihrer Organisation eingebunden?	OK	KO	N/A
17	Gibt es Alternativen für die zugelieferten Produkte oder Dienstleistungen?	OK OK	KO	N/A
18	Existieren geeignete, dokumentierte Vorgaben zur Absicherung der Supply Chain?	OK	KO	N/A
19	Sind Vorgaben für die Auswahl vertrauenswürdiger Zulieferer festgelegt?	OK	KO	N/A
20	Wird regelmäßig ein Supply-Chain Risk Assessment von Ihrer Organisation durchgeführt?	OK	KO	N/A
21	Wird regelmäßig ein Risikoassessment bzw. eine Lieferantenüberprüfung	OK	KO	N/A

	Ihrer externen Partnerinnen bzw. Partner durchgeführt und fordert Ihre Richtlinie für das Management von Lieferantenbeziehungen, dass Ihre Zulieferer dies auch für deren Zulieferer abwickeln?			
22	Wird regelmäßig ein Risikoassessment über externe Produkte und Dienstleistungen durchgeführt?	OK	KO	N/A
23	Existiert ein Konzept für die Einbindung externer Partnerinnen bzw. Partner anhand von verwalteten Berechtigungen, die für die durchzuführenden Tätigkeiten notwendig sind?	OK	KO	N/A
24	Existiert ein Konzept für den sicheren Datenaustausch insbesondere zwischen Ihrer Organisation und mit Dritten?	OK	KO	N/A
25	Existiert ein Konzept zur sicheren Einbindung von zugelieferten Bausteinen, Systemen Produkten oder Dienstleistungen die von Externen bezogen werden?	OK	KO	N/A
26	Existiert ein Verfahren zur Sicherheitsüberprüfung von externen Zulieferern das eine Sicherheitsüberprüfung vor dem Bezug der Leistung oder vor der Anstellung des externen Dienstleisters ermöglicht?	OK	KO	N/A
27	Existiert ein Konzept zum organisationsübergreifenden Umgang mit Sicherheitsvorfällen mit Ihren Zulieferern bzw. mit deren Zulieferern?	OK	KO	N/A
28	Überprüft Ihre Organisation vergebene Berechtigungen in regelmäßigen Abständen auf Ihre Aktualität?	OK	KO	N/A
II	PHYSISCHE MASSNAHMEN			
29	Existiert ein Konzept für die sichere Übergabe von Anlieferungen?	OK	KO	N/A
30	Werden Anlieferungen in geeigneter Form dokumentiert?	OK	KO	N/A
31	Existiert ein Konzept für die sichere Auslieferung von Waren, Dienstleistungen, Produkten oder Bausteinen?	OK	KO	N/A
32	Existieren Vorgaben zur sicheren Verwendung von (speziell mobilen) Endnutzengeräten vor allem auch in Bezug ihre Verwendung außerhalb der Organisation?	OK	KO	N/A